# Network Centric Operations Industry Consortium Inc.

**NCOIC Response to *NIST Request for Information – Developing a Framework to Improve Critical Infrastructure Cybersecurity* -- Federal Register / Vol 78, No. 38, Tuesday Feb 26, 2013**

April 8, 2013

Sent via email to: cyberframework@nist.gov

The following required information is provided:

1. Full company name: Network Centric Operations Industry Consortium Inc (aka NCOIC)

2. Business Address: 1301 Dove Street, Suite 890, Newport Beach CA 92660

3. Point of Contact: Carl Schwab, NCOIC Executive Director, Telephone (714) 878-2702, email carl.schwab@ncoic.org

4. ***Developing a Framework to Improve Critical Infrastructure Cybersecurity***

***NCOIC Response to NIST Request for Information – Developing a Framework to Improve Critical Infrastructure Cybersecurity* -- Federal Register / Vol 78, No. 38, Tuesday Feb 26, 2013**

**Purpose:** The Network Centric Industry Consortium (NCOIC) is responding to this RFI to inform NIST of on-going NCOIC activities that may be immediately useful and financially beneficial to NIST in carrying out its plan for developing the Cybersecurity Framework as described in the Federal Register posting. This paper addresses the subject from the collective perspective of the consortium based on its experience in pursuing similar objectives and goals for interoperability as those laid out by the NIST for cybersecurity. It is anticipated that individual member companies of the NCOIC will provide separate submittals addressing one or more of the NIST identified information topics of interest; and those submittals will provide greater detail on subjects that directly relate to their individual company needs and cybersecurity challenges.

**Introduction**: The NCOIC www.ncoic.org is an international not-for-profit organization whose goal is to collaboratively facilitate the adoption of existing and emerging open technical standards to achieve interoperability. The NCOIC mission is to facilitate interoperability and innovation across the spectrum of joint, inter-agency, inter-governmental, and multi-national industrial and commercial operations. NCOIC's experience and organizational structure for carrying out its mission may be useful in achieving similar goals and objectives for NIST with the focus directed toward cybersecurity. Within the NCOIC, interoperability and cybersecurity are generally seen as mutually prerequisite conditions. One should not expect to achieve cross domain interoperability if the enterprise does not have cybersecurity and vice versa; each condition is recognized prime requirement in achieving a reliable, functioning critical infrastructure. The NCOIC wants to be part of the NIST collaboration process used to define and develop the Cybersecurity Framework and is ready to share its experience and lessons learned on how to bring that collaboration about in a voluntary environment to achieve the consensus needed.


**Figure 1, NCOIC at a Glance**

**Activities Relevant to NIST Cybersecurity Framework:** Presently, the NCOIC is actively engaged in the following activities addressing similar issues and areas of concern identified in the NIST RFI:

1. **NCOIC Voice of Industry (VOI) Review and Perspective.**

NCOIC has an existing, organizational structure that has proven to be effective in bringing industry together with government agencies and academia to address complex challenges where there is diversity in perspectives and differences in the desired outcome. A key lesson learned is that it takes time to build-up trust in the organizational structure and processes used to share information and assemble a cumulative perspective; it doesn't happen quickly. The NCOIC organization, its collaborative processes, and past experiences would be useful and beneficial to the NIST in this regard as they have established that trust. While facilitating the adoption of existing and emerging open technical standards to achieve interoperability, the NCOIC has been supportive of policies that open opportunity for innovation, adaptation and new technology without compromising the hard-earned competitive advantage that comes with a company's intellectual property. Since its inception, the NCOIC has worked to earn the trust of its membership and has the skills needed to successfully bring representatives from across multiple user domains together to help identify priorities, requirements, capabilities, shortfalls and risks related to achieving sufficient cybersecurity for all stakeholders.

As an international organization chartered in the United States, the NCOIC is comprised of 55+ companies (such as Lockheed Martin, Boeing, IBM, Raytheon, EADS, and Thales) including a number of Fortune 500 companies and government FFRDC's as active members. The resulting breadth and depth of the resources available to NCOIC are extensive and provide a Voice of Industry (VOI) perspective for government customers; this independent review of the proposed Cybersecurity Framework should be an immediate benefit to NIST in defining and developing a workable framework to improve critical infrastructure Cybersecurity. Using the NCOIC established organizational structure, VOI reviews, and collaboration processes will help get the job done within the compressed timeline & schedule. As will be shown, the NCOIC organization and its membership have a shared history of helping government agencies meet their mission. NCOIC participation in the NIST project will include experienced engineers, technical personnel, and business partners to work the problem from a business approach in identifying open standards and best commercial practices to achieve cybersecurity across multiple domains.

## 2. Collaborative Tools.

Through its membership, the NCOIC has developed a set of net centric interoperability tools which could be useful in identifying and selecting the initial set of open standards needed to shape and develop the cybersecurity framework to improve critical infrastructure cybersecurity.


**Figure 2, NCOIC SCOPE Model Enables Practical Analysis of Enterprise Breath**

The NCOIC System-of-Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) model uses a workshop forum and has proven to be an effective collaborative, assessment tool for identifying and selecting standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address interoperability. The SCOPE model, with its proven track record with other government agencies, including the US, Australia, and NATO organizations, has the potential to be an excellent forum for bringing industry, government and academia together to achieve the same objectives for developing the Cybersecurity Framework.

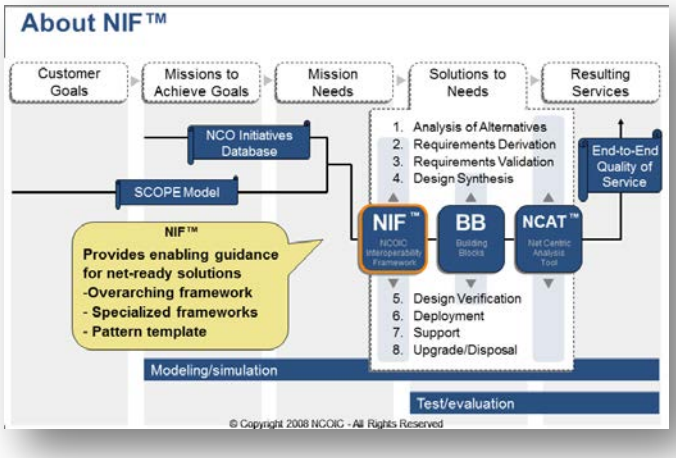


**Figure 3, NCOIC Assists Customers in Obtaining Interoperable, Secure Solutions**

An additional tool, known as the NCO Interoperability Framework (NIF™) provides overarching architectural guidance about the development of net-enabled systems. This architectural framework helps system architects and system engineers to design interoperable products and architectures, by supporting them with resources such as patterns, principles and methodologies. The information provided by the NIF complements reference architectures being developed by various civil and military entities

(departments, ministries, services), including NIST own Enterprise Architecture Framework. The NIF also complements systems engineering processes and tools used by other engineering firms and associations. Thus, NIF affords interoperability guidance that allows a firm to develop system elements/nodes that are interoperable with system elements/nodes that other firms are developing. Collectively, these NCOIC tools have the potential to significantly expedite the NIST efforts to define and develop the Cybersecurity Framework in an environment where No "One Size Fits All."

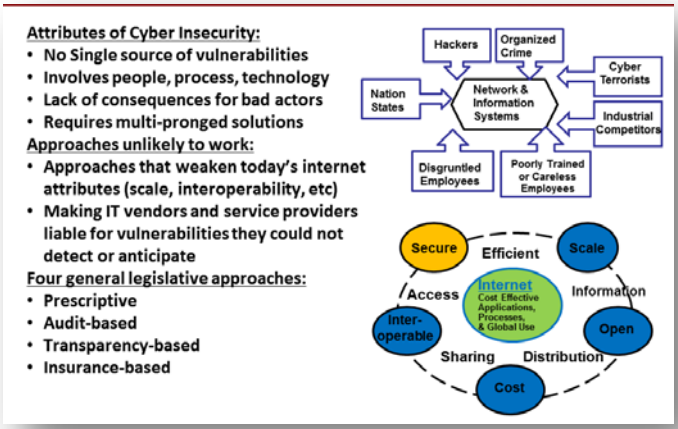


**Figure 4, Cybersecurity Landscape Study and Gap Analysis**

## 3. NCOIC Cybersecurity Landscape Study and Discovery Process.

Through its own Cybersecurity Integrated Product Team (IPT), NCOIC has initiated a study of the US cybersecurity landscape of current standards, policies, regulations and best practices identified by members representing the views of associated actors and stakeholders. This on-going activity is aimed at identifying key factors that either encourage or imped industry investment in cyber defense; and, to date, it has produced a growing database of 300+ cybersecurity related artifacts; i.e., standards, best practices, regulations, etc. As part of its participation in the NIST activity, NCOIC is prepared to make this study and its associated database available to NIST and other participating practitioners working related cybersecurity initiatives.

In response to an NCOIC Advisory Council inquiry, the Cybersecurity IPT is currently working to formalize a repeatable Cybersecurity Discovery Process to identify top level technologies, policies and procedures that either inhibit or enable secure, cross domain interoperability. Working with the NIST team, the NCOIC will demonstrate use of the Discovery Process to identify how national, regional, and local policies impact stakeholder ability to connect and interact with non-traditional partners; which standards and policies have the highest current value; and which market incentives will yield the highest industry investment to protect the critical infrastructure.

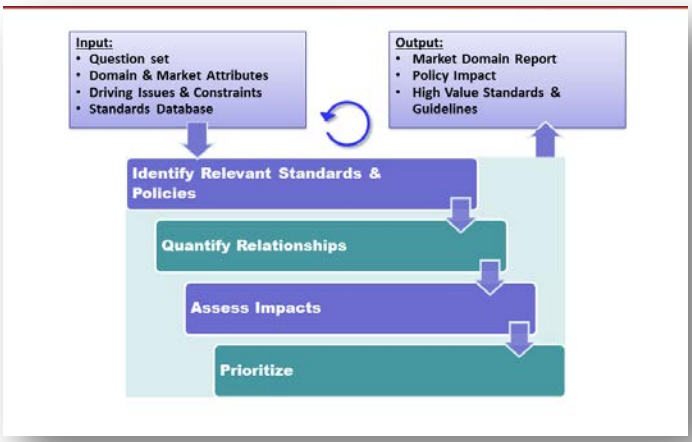


**Figure 5, Cybersecurity Discovery Process**

This activity aims to make it possible for member companies and customers to assess what is known and what is unknown; where security currently exists and where there are gaps in coverage. It is anticipated that using NCOIC discovery process, member companies and customers will be able to take into account the relationships between standards, policy, and business models; and scope the impact of both supporting and opposing positions to determine their investment strategy.

4. **The Value of Standing-up a Demonstration Test-bed Environment**.

The NCOIC is familiar with and endorses the layered NIST Enterprise Architectural (EA) framework model and has employed it to establish operational baselines in the past. It has also served as the foundation for establishing the NCOIC four level interoperability matrix which was the centerpiece of the 2010 Lab Interoperability demonstration, crossing four international borders and involving the participation of seven major companies at eight separate locations. In a more recent use, the NIST EA framework provided a baseline for the architectural analysis work done by NCOIC for the NATO Communications and Information Agency (NCI Agency). NCOIC was asked to take a holistic view of NATO IT organization and requirements needs, with the aim of bringing all NATO into a single enterprise Information and Communications Technology (ICT) structure. Using the NIST architectural model as a starting point, the NCOIC laid out an analysis approach (Figure 6) for assessing the likelihood of achieving the level of homogeneity needed to realize the savings goal sought-after through consolidation of the infrastructure and application spaces, as well as, consolidation of service management and control domain operations.

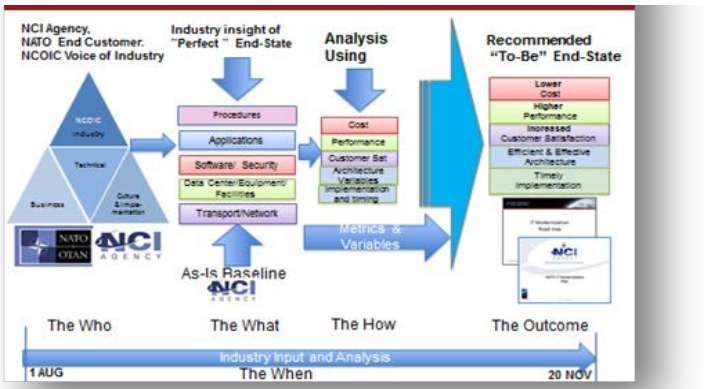


**Figure 6, NCOIC Architectural Analysis Process for NCIA**

Currently, the NCOIC is in the process of working on the second cycle of a contract for the National Geospatial-Intelligence Agency (NGA) regarding geospatial data movement in a multi cloud environment. As part of the infrastructure activity NCOIC and its members are implementing cloud security capabilities to include identity management and data security. The activity is a demonstration environment that enables new capabilities to be activated along with infrastructure systems, user applications and data structures. In fulfilling its contract, the NCOIC stood-up a demonstration - test bed environment using a federated cloud infrastructure to explore cloud computing concepts. The agency had requested NCOIC propose a solution that would demonstrate the capability to create a dynamic GEOINT analytic environment and enterprise domain for use by NATO, coalition, other allies, and Non-Government Organizations; and, service their needs during an international humanitarian crisis such as Haiti or a man-made disaster.

Starting with its international lab interoperability demonstration in 2010 and continuing through to its most recent NGA cloud demonstration environment using a federated cloud environment, the NCOIC has gained a fair amount of experience in how to bring together multiple vendors, including competitive developers to work in a common environment on new challenges; and, do it in a fashion that ensures the intellectual property of each participant is protected. With those considerations in-place, the NCOIC has found that use of the demonstration test-bed environment to be an effective means for exploring and validating new concepts and

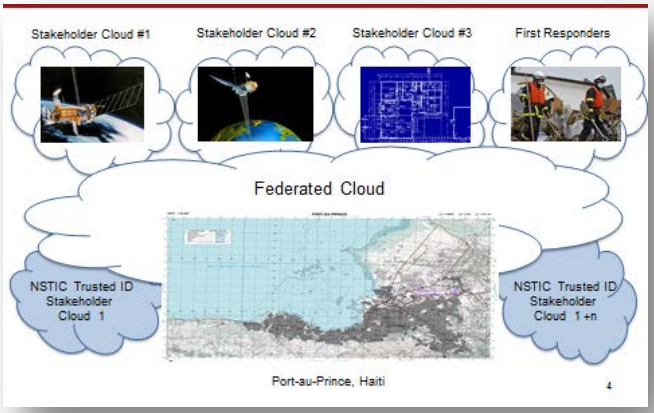


**Figure 7, Federated Cloud Demonstration-Test Environment with Disaster Response Scenario**

capabilities where multiple cross domain players are involved. The NCOIC organization has the experience and established processes for assembling a demonstration- test bed environment; and is prepared to assist NIST in procuring the technical services needed to a similar environment for cybersecurity.

The on-going NCOIC activity with NGA provides a real time working model on how to establish and build the demonstration–test bed environment for exploring and testing the impact and/or benefit to cybersecurity associated with using a federated cloud environment. Additionally, the disaster response scenario and growing database used in the NGA effort would provide a neutral test environment for exploring cybersecurity challenges. With the diverse set of responders involved in an international recovery effort, the large natural disaster provides a ready-made set of diverse services involved in collecting, transferring, and processing data with variable degrees of sensitivity required. It has multiple cross domain processes using new technology and legacy systems supporting an emergency-response scenario with fixed, transportable, and mobile users participating. Lessons learned and knowledge gained from the NGA initiative and other contract activity completed by the NCOIC can be made available to the NIST team working on the development of the Cybersecurity Framework.

**In Summary,**

NCOIC shares the government's concern regarding the dependency of national and economic security on having a reliable, functioning critical infrastructure which must be defended against an increasing, malicious cyber activity. And, the NCOIC is ready to assist NIST in achieving the voluntary collaboration needed to develop a framework to improve critical infrastructure cybersecurity. The NCOIC believes that its corporate history and focus on interoperability will prove to be beneficial to NIST in ferreting out the standards, methodologies, procedures, and processes needed to align policy, business practices and technological approaches capable of addressing the cyber risk. In accomplishing its mission of promoting interoperability across industry and government, the NCOIC has developed the organizational forum, established practices, and learned experience needed to collaboratively facilitate voluntary adoption of existing and emerging open technical standards to achieve interoperability. By sharing that knowledge with NIST, the combined team will have an advantage in successfully identifying the standards, methodologies, and procedures needed for the Cybersecurity Framework.

The NCOIC membership, with its broad cross-section of Industry, government and academia representatives, has the experience, technical capability and knowledge needed to address and identify the information being sought out. As the NIST Director Patrick Gallagher said, ***"By collaborating with industry to develop the framework, we will better protect our nation from the cybersecurity threat while enhancing America's ability to innovate and compete in a global market."***[i] Bottom line: NCOIC wants to be part of that collaboration process and is looking forward to working with the NIST team.

---

[i] http://www.commerce.gov/news/press-releases/2013/02/13/national-institute-standards-and-technology-initiates-development-new

Other References:
*https://www.ncoic.org/technology/deliverables/scope/*
https://www.ncoic.org/technology/deliverables/ifg/